WEBER STATE UNIVERSITY INFORMATION TECHNOLOGY DIVISION	**MOBILE DEVICE STANDARDS & GUIDELINES**	Standard #	2012-IT-SG-1
		Date Approved:	
		Authors:	Vern Morgan, Jonathan Karras, Andrea Grover, Bret Ellis

DRAFT

I. REFERENCES

Understanding and identifying Private and Public Information

PPM 10-1, Information Security Policy

PPM 10-2, Acceptable Use Policy for Computing and Network Resources

PPM 10-6, Mobile Device Policy

II. DEFINITIONS

Mobile Device – Any handheld or portable computing device including, but not limited to, a smartphone, PDA, or tablet.

Sensitive information – Any information that, if released to the public, could be used to cause harm or damage to either an individual or the university. Such information could include Social Security Numbers, driver's license information and individual financial information (such as credit card numbers, bank account numbers, or financial statements). Sensitive information is used in this document to include high-risk, restricted and confidential information. See PPM 10-1, Information Security Policy for definitions of these information classifications.

PIN – Personal Identification Number. This can be any combination of numbers usually a minimum of four that is used to unlock a device.

Encryption – The use of software or hardware code to make data unreadable unless the device is presented with the correct password or PIN. Most mobile devices include this feature but require the user to enable it.

Remote wipe – The ability to erase all of the data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

Virus – A computer program that is usually hidden within another seemingly innocuous program that has the function of stealing or destroying data or causing any number of unwanted system behaviors.

Malicious software – Often called malware, this is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.

Anti-virus software – Software designed to detect and/or remove malicious software and viruses from a computer system.

Data Security Steward – Individuals within the different University organizations, appointed by the College dean or Division head, who are points of contact for security violations or issues and a general reference within their work centers for Information Security topics.

Strong Password – A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and characters. Strong passwords do not include phrases, names, or other types of dictionary words.

Security Patch – A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most mobile devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

III. STANDARDS

The items listed below are the minimum security controls that need to be utilized for mobile devices used to access the Weber State University network resources for the purpose of processing sensitive information pertaining to anyone other than the user. Adhering to these standards will insure a minimum level of data security.

A. All mobile devices, University or personally owned and utilizing University network resources, will be subject to the provisions of PPM 10-2, Acceptable Use Policy for Computing and Network Resources.

B. If possible, all devices will be updated to the latest device operating system with the latest security patches.

C. All applications (apps) will be updated with the latest security patches.

D. All devices will be configured with a PIN, pattern, or password enabled lock screen configured to activate at no more than 5 minutes of inactivity.

E. All devices with built in encryption capability will have onboard device encryption enabled.

F. All devices will have remote wipe enabled either through mobile sync, a third party app or the manufacturer's website.

G. All devices that have been used to store, access and/or process sensitive information will be wiped to remove such data before they are transferred to someone else through sale or gifting.

DRAFT

H. In the event that a device that has been used to store, access and/or process sensitive information becomes lost, stolen or compromised, the owner must comply with section V part H of PPM 10-1, Information Security Policy. For a listing of the Data Security Stewards by division, please refer to the Data Security Stewards document. Additionally, the user must contact the IT Service Desk (801-626-7777) to request remote wiping through Mobile Sync if that service is utilized on the device.

GUIDELINES

The standards outlined above will ensure a minimum level of security for mobile devices and prevent, in most cases, data compromise due to lost or misplaced devices. Network users are also encouraged to review the following guidelines and be cognizant of them as additional security measures then can implemented to enhance the protection of their mobile devices.

A. Make sure you are aware of the location of your mobile device at all times. Do not leave it unattended.

B. Setup your device to backup your data at regular intervals. This will increase your confidence to use the wipe feature if you ever suspect your device to be lost or stolen.

C. Consider using a password instead of a pin or pattern for your lock screen. Passwords, especially strong passwords, are much more secure.

D. If possible, configure your device to automatically wipe its data after a preset number of unsuccessful password attempts.

E. Do not allow someone who is not authorized access to the university network to use your device if it is used to process sensitive information.

F. Install anti-virus software.

G. Learn how your mobile device functions. Not all users are aware that when you open an attachment from email most devices will store a copy of this attachment in the download folder. Consult your user manual and other sources to learn how your device handles data.

H. It is good practice to use your mobile device only for transitory storage of sensitive data. You should delete any sensitive data stored on your device immediately after your work with it is complete.

DRAFT